Security CLI Reference

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

CLI commands for configuring and monitoring security.

Security CLI Templates

The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allows you to configure intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, Cisco SD-WAN Manager enables pushing vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in Cisco IOS XE syntax.

Table 1: Security Policy for UTD

CLI Template Configuration	Configuration on the Device
policy zone internet vpn 0 ! zone zone1 vpn 1 ! zone zone2 vpn 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text "<![CDATA[<h3>Access" to the requested page has been denied]]>" target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open ! ! !	

CLI Template Configuration	Configuration on the Device
	ip access-list extended fw_policy-seq-1-acl_ 11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_ match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy class fw_policy-seq-1-cm_ inspect ! class class-default pass ! ! object-group service fw_policy-seq-1-service-og_ ip ! parameter-map type inspect-global alert on log dropped-packets multi-tenancy vpn zone security ! parameter-map type umbrella global token A5EA676087BF66A42DC4F722C2AFD10D00256274 dnscrypt vrf 1 dns-resolver umbrella match-local-domain-to-bypass ! ! zone security internet vpn 0 ! zone security zone1 vpn 1 ! zone security zone2 vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2 service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0

CLI Template Configuration	Configuration on the Device

	guest-interface 0
	  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
	  !
	  app-vnic gateway1 virtualportgroup 1 guest-interface 1
	  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
	  !
	  start
	  !
	  utd multi-tenancy
	  utd engine standard multi-tenancy
	  web-filter block page profile block-url_filter
	  text <\![CDATA[Access to the requested page has been denied Please contact your Network Administrator]]>
	  !
	  web-filter url profile url_filter
	  categories block
	  games
	  !
	  block page-profile block-url_filter
	  log level error
	  reputation
	  block-threshold moderate-risk
	  !
	  !
	  threat-inspection profile intrusion_policy
	
	  threat protection
	  policy connectivity
	  logging level err
	  !
	  utd global
	  !
	  policy utd-policy-vrf-1
	  all-interfaces
	  vrf 1
	  threat-inspection profile intrusion_policy
	
	  web-filter url profile url_filter
	  exit
	  !

Security Monitoring Commands

- **show control connections**